4 ESERCIZI SVOLTI

Giovanni Ferranti <gyofer@yahoo.it>

ESERCIZIO n°1:

Trovare le ultime due cifre di 3^{1234}.

Il trucco da applicare in questi casi è il seguente: si fa una congruenza modulo 10 se è richiesta l'ultima cifra (in base 10), modulo 100 se sono richieste le ultime due, module 1000 per le ultime tre e così via...

$3^{1234} \equiv x(100)$ Si nota che $(3,100) = 1$

$\varphi(100) = \varphi(2^2) \cdot \varphi(5^2) = 40$

$1234 = 40 \cdot 30 + 34$

$3^{1234} \equiv 3^{\varphi(100)\cdot 30+34} \equiv x(100)$

$3^{\varphi(100)\cdot 30} \cdot 3^{34} \equiv x(100)$

$\diagdown$

1

Si è pertanto ridotto $3^{1234} \equiv x(100)$ a $3^{34} \equiv x(100)$ dividendo il primo esponente per $\varphi(100)$ e trovandone il resto. Se non ci fosse stato resto x=1 in Z_{100} ed avrei già finito.

Per il teorema Cinese del Resto

$$\begin{cases} 3^{34} \equiv x(5^2) \\ 3^{34} \equiv x(2^2) \end{cases}$$

$3^{34} \equiv x(25)$

$\varphi(25) = \varphi(5^2) = 20$

perciò si sa che

$3^{\varphi(25)+14} \equiv x(25)$

$3^{\varphi(25)} = 1 \cdot 3^{14} \equiv x(25)$

$3^{14} \equiv x(25)$

NOTA!! Non si può ridurre ulteriormente l'esponente per due motivi:

1) L'esponente è minore del modulo;
2) Il M.C.D. tra 3 e 25 è diverso da 1.

Essendo $\left[3^{14}\right]_{25} = [4727969]_{25} = [19]_{25}$ $\quad 19 \equiv x(25)$.

Per quanto riguarda la seconda congruenza si ha:

$3^{34} \equiv x\left(2^2\right), \qquad \left(3,2^2\right) = 1$

$\varphi\left(2^2\right) = 2$ ma l'esponente 34 è un multiplo di 2, quindi si ha:

$1 \equiv x\left(2^2\right)$.

Si ha dunque il sistema:

$\begin{cases} x \equiv 19(25) \\ x \equiv 1(4) \end{cases}$ che si risolve facilmente e si ottiene $x \equiv 69(100)$.

ESERCIZIO n° 2:

$$\binom{n}{3} \equiv \binom{n}{4} \equiv 0(\mathrm{mod}\, 6)$$

Ciò corrisponde al seguente sistema:

$$\begin{cases} * \dfrac{n \cdot (n-1) \cdot (n-2)}{6} \equiv 0(\mathrm{mod}\, 6) \\ ** \dfrac{n \cdot (n-1) \cdot (n-2) \cdot (n-3)}{24} \equiv 0(\mathrm{mod}\, 6) \end{cases}$$

Per quanto riguarda la congruenza (*)

$n \cdot (n-1) \cdot (n-2) \equiv 0(\mathrm{mod}\, 36)$

Si vuole che 36 divida il numero $\binom{n}{3}$.
Se si prendono tre numeri consecutivi conviene calcolare le classi di congruenza mod $36 = 2^2 \cdot 3^2$.
Questo numero dev'essere divisibile per $2^2 \cdot 3^2$.
Per il Teorema Cinese si ha:

$$\begin{cases} n \cdot (n-1) \cdot (n-2) \equiv 0\left(\mathrm{mod}\, 2^2\right) \\ n \cdot (n-1) \cdot (n-2) \equiv 0\left(\mathrm{mod}\, 3^2\right) \end{cases}$$

Per quanto riguarda la prima congruenza si ha che:

Se $n \equiv 0(\mathrm{mod}\, 4)$ va bene.
se $n \equiv 1(\mathrm{mod}\, 4)$ idem.
se $n \equiv 2(\mathrm{mod}\, 4)$ idem.

se $n \equiv 3 (\mathrm{mod}\, 4)$ non va bene perchè avrei n dispari, n-1 pari ma divisibile solo per 2 e non per 4 e n-2 dispari.

Quindi si ha $n \equiv 0,1,2 (\mathrm{mod}\, 4)$.

Per quanto riguarda la seconda congruenza si ha che:

Se $n \equiv 0 (\mathrm{mod}\, 9)$ va bene.
se $n \equiv 1 (\mathrm{mod}\, 9)$ idem.
se $n \equiv 2 (\mathrm{mod}\, 9)$ idem.
negli altri casi non va bene!

Quindi si ha $n \equiv 0,1,2 (\mathrm{mod}\, 9)$.

Per quanto riguarda la congruenza (**)

$n \cdot (n-1) \cdot (n-2) \cdot (n-3) \equiv 0 (\mathrm{mod}\, 144)$ $\qquad$ $144 = 2^4 \cdot 3^2$

Per il Teorema Cinese del Resto si ha:

$$\begin{cases} n \cdot (n-1) \cdot (n-2) \cdot (n-3) \equiv 0 (\mathrm{mod}\, 2^4) \\ n \cdot (n-1) \cdot (n-2) \cdot (n-3) \equiv 0 (\mathrm{mod}\, 3^2) \end{cases}$$

Per quanto riguarda la seconda congruenza si ha che:

Se $n \equiv 0,1,2,3 (\mathrm{mod}\, 3^2)$ va bene.
se $n \equiv 4,5 (\mathrm{mod}\, 3^2)$ non va bene.
se $n \equiv 6 (\mathrm{mod}\, 3^2)$ va bene perchè si ha n=6 e (n-3)=3 e 6·3=18 che è divisibile per 9.
se $n \equiv 7,8 (\mathrm{mod}\, 3^2)$ non va bene perchè no si trova nessun elemento di $n \cdot (n-1) \cdot (n-2) \cdot (n-3)$ divisibile per 9 se n=7 o n=8.

Perciò $n \equiv 0,1,2,3,6 (\mathrm{mod}\, 3^2)$

Per quanto riguarda la prima congruenza si ha che:

Se $n \equiv 0,1,2,3 (\mathrm{mod}\, 16)$ va bene.
se $n \equiv 4,5,6 (\mathrm{mod}\, 16)$ non va bene.
se $n \equiv 8,9,10,11 (\mathrm{mod}\, 16)$ va bene.
se $n \equiv 12,13,14,15 (\mathrm{mod}\, 16)$ non va bene.

Quindi $n \equiv 0,1,2,3,8,9,10,11 (\mathrm{mod}\, 16)$

Da qui si determinano le soluzioni:

$$\begin{cases} \binom{n}{3} \equiv 0 (\mathrm{mod}\, 6) \Rightarrow \begin{cases} n \equiv 0,1,2 (\mathrm{mod}\, 4) \\ n \equiv 0,1,2 (\mathrm{mod}\, 9) \end{cases} \\ \binom{n}{4} \equiv 0 (\mathrm{mod}\, 6) \Rightarrow \begin{cases} n \equiv 0,1,2,3,6 (\mathrm{mod}\, 9) \\ n \equiv 0,1,2,3,8,9,10,11 (\mathrm{mod}\, 16) \end{cases} \end{cases}$$

Bisogna risolvere tutti i possibili sistemi.

ESERCIZIO n° 3:

Determinare il n° di soluzioni degli interi positivi con $x \leq 6300$ che verificano il sistema:

$$\begin{cases} (x,12) = (x,18) \\ 3^x \equiv 1 (\mathrm{mod}\, 7) \end{cases}$$

Per quanto riguarda la seconda congruenza si ha che:

$$3^x \equiv 1 (\mathrm{mod}\, 7) \Leftrightarrow x \equiv 0 (\mathrm{mod}\, 6)$$

$$(x,12) = (x,18)$$

$$12 = 2^2 \cdot 3$$

$$18 = 2 \cdot 3^2$$

Quindi il M.C.D. comune tra x, 12 e 18 può essere solo 2, 3 o 6.
un numero Non può essere 1 perchè x è multiplo di 6 (quindi non è primo).
È chiaro che:

$x \not\equiv 0 (\mathrm{mod}\, 12)$ e $x \not\equiv 0 (\mathrm{mod}\, 18)$

$x \not\equiv 0 (\mathrm{mod}\, 4)$ $\quad$ $x \not\equiv 0 (\mathrm{mod}\, 3)$ $\quad$ $x \not\equiv 0 (\mathrm{mod}\, 9)$ $\quad$ $x \not\equiv 0 (\mathrm{mod}\, 2)$

$$x \equiv 1,2,3 (\mathrm{mod}\, 4)$$

$$x \equiv 1,2 (\mathrm{mod}\, 3)$$

$$x \equiv 1,2,3,4,5,6,7,8 (\mathrm{mod}\, 9)$$

$$x \equiv 1 (\mathrm{mod}\, 2)$$

Si scartano le congruenze che non sono possibili:

essendo $x \equiv 0 (\mathrm{mod}\, 6)$ x è di sicuro un numero pari, perciò

$$x \not\equiv 1 (\mathrm{mod}\, 2)$$

$$x \not\equiv 1,3 (\mathrm{mod}\, 4)$$

inoltre poichè x=k6 si ha che:

$$x \not\equiv 1,2 (\mathrm{mod}\, 3)$$

$$x \not\equiv 1,2,4,5,7,8 (\mathrm{mod}\, 9)$$

Perciò rimane:

$$\begin{cases} x \equiv 0 (\mathrm{mod}\, 6) \\ x \equiv 2 (\mathrm{mod}\, 4) \\ x \equiv 3,6 (\mathrm{mod}\, 9) \end{cases}$$

Si hanno perciò due possibili soluzioni modulo 36 (poichè 36=[6,4,9]).

ESERCIZIO n° 4:

Determinare il n° degli interi positivi con $x \leq 4200$ che verificano:

$$x^8 \equiv x (\mathrm{mod}\, 35)$$

$$x^8 - x \equiv 0 (\mathrm{mod}\, 35)$$
$$x(x^7 - 1) \equiv 0 (\mathrm{mod}\, 35)$$

$$* \begin{cases} x(x^7 - 1) \equiv 0 (\mathrm{mod}\, 5) \\ x(x^7 - 1) \equiv 0 (\mathrm{mod}\, 7) \end{cases}$$

Per quanto riguarda la prima congruenza si ha che:

$x \equiv 0 (\mathrm{mod}\, 5)$ oppure $x^7 \equiv 1 (\mathrm{mod}\, 5)$

$x^7 \equiv 1 (\mathrm{mod}\, 5)$ $\qquad \varphi(5) = 4$

$x^3 \cdot x^4 \equiv 1 (\mathrm{mod}\, 5)$

$x^4 \equiv 1 (\mathrm{mod}\, 5)$

$x^{\varphi(5)} \equiv 1 (\mathrm{mod}\, 5) \Leftrightarrow (x,5) = 1$
cioè $x \not\equiv 0 (\mathrm{mod}\, 5)$ il che vuol dire
$x \equiv 1,2,3,4 (\mathrm{mod}\, 5)$

$x^3 \equiv 1 (\mathrm{mod}\, 5)$

$x \cdot x^2 \equiv 1 (\mathrm{mod}\, 5)$

$x \equiv 1 (\mathrm{mod}\, 5)$

$x^2 - 1 \equiv 0 (\mathrm{mod}\, 5)$
$(x+1) \cdot (x-1) \equiv 0 (\mathrm{mod}\, 5)$
$x \equiv 1 (\mathrm{mod}\, 5)$ oppure $x \equiv -1 (\mathrm{mod}\, 5)$

$$x^7 \equiv 1(\mathrm{mod}\,5) \Leftrightarrow \begin{cases} x \equiv 1,2,3,4(\mathrm{mod}\,5) \\ x \equiv 1(\mathrm{mod}\,5) \\ x \equiv 1,4(\mathrm{mod}\,5) \end{cases} \quad \text{contemporaneamente}$$

L'unica soluzione comune è $x \equiv 1(\mathrm{mod}\,5)$

Si unisce $x \equiv 1(\mathrm{mod}\,5)$ a $x \equiv 0(\mathrm{mod}\,5)$ in quanto per

$$x(x^7 - 1) \equiv 0(\mathrm{mod}\,5)$$

basta che $x \equiv 0(\mathrm{mod}\,5)$ oppure $x^7 \equiv 1(\mathrm{mod}\,5)$
cioè che $x \equiv 1(\mathrm{mod}\,5)$.

Quindi il sistema (*) diventa:

$$\begin{cases} x \equiv 0,1(\mathrm{mod}\,5) \\ x(x^7 - 1) \equiv 0(\mathrm{mod}\,7) \end{cases}$$

Per quanto riguarda la seconda congruenza si ha che:

o $x \equiv 0(\mathrm{mod}\,7)$ oppure $x^7 \equiv 1(\mathrm{mod}\,7)$.

Il primo caso è ovvio mentre il secondo no e si ha:

$$x^7 \equiv 1(\mathrm{mod}\,7) \qquad \varphi(7) = 6$$

$$x \cdot x^6 \equiv 1(\mathrm{mod}\,7) \Rightarrow \begin{cases} x \equiv 1(\mathrm{mod}\,7) \\ x^6 \equiv 1(\mathrm{mod}\,7) \end{cases}$$

$x^6 \equiv 1(\mathrm{mod}\,7) \Leftrightarrow (x,7) = 1$ cioè se $x \equiv 1,2,3,4,5,6(\mathrm{mod}\,7)$

$$\begin{cases} x \equiv 1(\mathrm{mod}\,7) \\ x \equiv 1,2,3,4,5,6(\mathrm{mod}\,7) \end{cases}$$

va bene solo $x \equiv 1(\mathrm{mod}\,7)$ che è anche l'unica soluzione in comune.

Alla fine il sistema (*) diventa:

$$\begin{cases} x \equiv 0,1(\mathrm{mod}\,5) \\ x \equiv 01(\mathrm{mod}\,7) \end{cases}$$

Si hanno perciò quattro soluzioni modulo 35.